Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): NAI1P482/01.122.01

I hereby certify that this correspondence is being e-filed with the USPTO on November 14, 2007

Signature: /Dana Chan/

Typed or printed name: Dana Chan

Application Number	Filed
10/023,852	12/21/2001

First Named Inventor: Paul Nicholas Gartside

Art Unit	Examiner
2131	Besrour, Saoussen

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/KEVINZILKA/
Signature

Kevin J. Zilka
Typed or printed name

408-971-2573
Telephone number

November 14, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

REMARKS

The Examiner has rejected Claims 1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38, 40-47 and 49-50 under 35 U.S.C. 103(a) as being unpatentable over Nambu (U.S. Patent Publication No. 2002/0124182), in view of Hershberg et al. (U.S. Patent Publication No. 2003/0022657). Applicant respectfully disagrees with such rejection.

With respect to the independent claims, the Examiner has relied on paragraph [0072] - [0074] from the Nambu reference to make a prior art showing of applicant's claimed "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in the independent claims).

More specifically, the Examiner has asserted that "it is known within existing malware definition data to include information that classifies the malware items using classes." However, applicant respectfully disagrees and notes that the excerpts relied on by the Examiner merely teach that a "maintenance server... registers and manages the information of new types of viruses" and that "[t]he maintenance server... receives and stores updated vaccine software (including scan engines) and pattern data files" (paragraph [0072] – emphasis added). Further, the excerpts teach that "support computers... of the vaccine software makers may upload vaccine software and pattern files to the maintenance server" and that [t]he maintenance server... is connected to various user terminals" (paragraphs [0073]-[0074] – emphasis added).

However, registering and managing new virus types, receiving and storing updated vaccine software and pattern data files, and uploading vaccine software to a server which is connected to user terminals, as in Nambu, does not teach "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed by applicant. Additionally, it appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested (See MPEP 2112).

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraph [0071] in Nambu "states that the pattern files can be referred to as signature files or virus definition files, where it is a code of particular virus, [which is] interpreted by [the] examiner as the class of malware." The

Examiner has also argued that paragraphs [0075]-[0078] state "that the maintenance server stores information on all the related user terminals based on the user-related information" and that "it provides the terminals with updated vaccine and pattern files." Further, the Examiner has argued that paragraph [0083] "discloses protecting against the new virus, which the device is to be protected against," that paragraph [0089] "states that the information 54a and 54b...include information of the user's device, such as applied pattern name for that user device," and that paragraph [0095] "states that the new anti-virus program reads user information and acquires the software related information from each use[r], including [the] pattern file."

Applicant respectfully disagrees and asserts that paragraph [0071] in Nambu only discloses pattern files which may be referred to as signature files and virus definition files, where such pattern files are each associated with a new virus (see paragraph [0072]). Further, the Examiner has even admitted that Nambu teaches "a code of a particular virus," as noted above. Clearly, a pattern file that is associated with a particular virus, as in Nambu, does not meet applicant's claimed "one or more classes of malware" (emphasis added), as claimed. Additionally, applicant respectfully asserts that merely "install[ing]... pattern files...[to prevent] the terminal from being infected by the new virus" (paragraph [0083]), as relied on by the Examiner, fails to specifically teach "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed.

Additionally, with respect to the independent claims, the Examiner has relied on paragraphs [0075], [0077] and [0078] from the Nambu reference to make a prior art showing of applicant's claimed "generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully points out that the excerpts relied on by the Examiner merely teach that a "maintenance server... stores information related to the user terminals" and "provides the terminals... with updated vaccine software and pattern files" (emphasis added). Additionally, the excerpts teach that "[t]he maintenance server 41 stores vaccine software and pattern files" (emphasis added). Further, the excerpts teach that "[t]he first information file... functions as a new virus countering information memory and stores vaccine software information" and that "[t]he second information file... stores the present condition of the user terminal" (emphasis added).

However, merely storing vaccine software and pattern files and information, in addition to storing the present condition of a user terminal, as in Nambu, fails to disclose "generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed by applicant. Clearly, merely storing pattern files and information, as in Nambu, simply fails to even suggest "classes of malware threat against which said mobile computing device is to be protected" (emphasis added), in the manner as claimed by applicant.

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraphs [0093], [0095] and [0096] state "software designated information from each user." Applicant respectfully disagrees. First, applicant respectfully asserts that simply alleging that the Nambu reference discloses "information from each user," as noted by the Examiner, fails to even suggest "classes of malware threat," as applicant claims. Second, applicant respectfully asserts that simply disclosing "stor[ing] various types of information" (paragraph [0093]), "software-related information from each user (e.g., hardware information, identification number, vaccine software information, designation of applied vaccine, applied pattern file name)" (paragraph [095]), and that "pattern files may be provided" (paragraph [0096]), as in Nambu, fails to even suggest "classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed. As noted above, a pattern file in Nambu only relates to a particular virus, and thus does not meet applicant's claimed "classes of malware threat" (emphasis added), as claimed.

Further, with respect to the independent claims, the Examiner has relied on paragraphs [0074], [0075], and [0077] from the Nambu reference to make a prior art showing of applicant's claimed technique "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully notes that the excerpts relied on by the Examiner merely disclose that "[t]he maintenance server... is connected to various user terminals" (paragraph [0074] – emphasis added), that "[t]he maintenance server 41 stores information related to the user terminals" (paragraph [0075] –

emphasis added), and that "[t]he maintenance server... stores vaccine software and pattern files... that are received from the vaccine software makers" (paragraph [0077] – emphasis added).

However, merely storing information related to user terminals, in addition to storing vaccine software and pattern files, as in Nambu, fails to teach a technique "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added), as claimed by applicant. Clearly, storing information relating to user terminals and providing updated vaccine software and pattern files, as in Nambu, simply fails to suggest "transfer[ing] computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added), as claimed by applicant.

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraph [0083] in Nambu "states transferring vaccine software and pattern file." Applicant respectfully disagrees. As argued above, applicant respectfully asserts that the pattern file in Nambu only relates to a particular virus (see paragraph [0072]), which simply does not even suggest "transfer[ing] computer files and corresponding threat data identifying one or more classes of malware threat," especially where such classes of malware threat particularly include those "to which each of said mobile computing devices is **vulnerable**" (emphasis added), as claimed by applicant.

Further still, with respect to the independent claims, the Examiner has relied on paragraphs [0078], [0081] and [0108] from the Nambu reference to make a prior art showing of applicant's claimed technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully points out that the excerpts relied on by the Examiner merely disclose that "[t]he first information file... functions as a new virus countering information memory and stores vaccine software information" and that "[t]he second information file... stores the present condition of the user terminal" (paragraph [0078] - emphasis added). Additionally, the excerpts teach that the "new anti-virus processing program... acquires the vaccine software-related information" as well as "new virus

countering information." Further, the excerpts teach that "[t]he maintenance server... determines whether the vaccine software and pattern data files presently used... are capable of countering a new virus" and that "[b]ased on the determination, the resource distribution program... distributes to the user terminals... vaccine software and pattern files... that have been updated to counter the new virus" (emphasis added).

However, merely acquiring vaccine and virus countering information, determining whether a vaccine is capable of countering a new virus, and distributing vaccine software based on the determination, as in Nambu, fails to suggest a technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (emphasis added), as claimed by applicant. Clearly, distributing vaccine software based on the determination if the vaccine is capable of countering a new virus, as in Nambu, simply fails to even suggest that "one or more classes of malware threat... are chosen according to classes of malware threat known to pose a problem to said mobile computing device" (emphasis added), in the manner as claimed by applicant.

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraphs [0089] and [0100]-[0103] in Nambu state "determining that the vaccine software and data pattern file have not been updated for new virus, then based on the determination obtaining up to date vaccine from user information."

Applicant respectfully disagrees. Paragraphs [0089] and [0100]-[0103] in Nambu, as relied on by the Examiner, merely relate to "information of the user's terminal, such as...designation of applied vaccine" which designates whether "user A wishes to receive updated vaccine, which includes that of other makers" (see paragraph [0089]), such that if "user A wishes to obtain the most updated vaccine (including that of other makers)...countering information...of the B vaccine software maker [is read]" (see paragraph [0103]). Clearly, simply determining whether a user wishes to receive an updated vaccine from another vaccine software maker, as in Nambu, fails to even relate to "classes of malware threat" (emphasis added), let alone specifically teach "one or more classes of malware threat... are chosen according to classes of malware threat **known to pose a problem to said mobile computing device**" (emphasis added), in the manner as claimed by applicant.